Version: 2020.1
Version date: 1 March 2020

Addendum to the Agreement with reference _____
DATA PROCESSING AGREEMENT LEASEWEB AS PROCESSOR

PARTIES:

1. [……], a private company with limited liability, having its registered seat at [……] and its office at [……]at the [……] ("**Customer**" or "**Controller**");

and

2. **LEASEWEB USA, INC.**, a Delaware Corporation, with its registered office at 9301 Innovation Drive/Suite 100, Manassas, VA 20110, the United States of America ("**Leaseweb**" or "**Processor**");

Customer/Controller and Leaseweb/ Processor will also individually be referred to as "**Party**" and together as "**Parties**".

INTRODUCTION:

A. Leaseweb is part of one of the world's largest hosting brands, providing Infrastructure-as-a-Service (IaaS) hosting solutions to its customers worldwide, ranging from SMBs to enterprises (the "**Services**"). The Services include Public Cloud, Private Cloud, Dedicated Servers, Data Storage, Cybersecurity, Colocation, Managed Hosting, and Hybrid Solutions.
B. Parties entered into the Agreement pursuant to which Leaseweb shall provide certain Services to Customer, which Services are indicated on the Order Form(s) or the Order Confirmation into order(s) with respect to the provision the Services.
C. In the performance of Leaseweb's obligations under the Agreement, in particular for the purpose of storage on behalf of the Customer, Leaseweb and its Affiliates shall Process Personal Data for or on behalf of the Customer. Parties acknowledge and agree that with regard to the Processing of Personal Data on the Customer's behalf, the Customer is the Controller, and Leaseweb is the Processor. Furthermore, Parties are aware that Leaseweb's role as Processor as IAAS provider is limited.
D. In order to comply with the relevant Data Protection Legislation, in particular the GDPR ("**Data Protection Legislation**"), with respect to the Processing of Personal Data by Leaseweb, Parties agree upon the conditions as set forth in this Data Processing Agreement ("**DPA**").

HAVE AGREED AS FOLLOWS:

1. DOCUMENT STRUCTURE, DEFINITIONS AND INTERPRETATION

1.1 In addition to the terms and conditions of the Agreement, the terms and condition set forth in this DPA shall apply to Processing of Personal Data.

1.2 The definitions and guidelines for interpretation are set out in the General Conditions, the Support and Service Level Schedule, the Leaseweb Policies and the Services Specification and in addition to that, the definitions set forth in this DPA shall apply.

1.3 In the event of a dispute between this DPA and the General Conditions, the Support and Service Level Schedule, the Leaseweb Policies and/or the Services Specification, the contents of this DPA shall prevail, except for an Order, which will always prevail.

2. PROCESSING

2.1 Processor shall Process Personal Data of Controller. The details of Processing are set forth below:

Data Subject:	Controller is aware that Leaseweb does not control and never acts as controller of any Personal Data and content of Customer transmitted over Controller's Network. The Data Subject can be anyone (Controller's employees, suppliers, prospects, customer or end users) and Controller acknowledges that Leaseweb has no information with respect hereto.
Processing purposes:	Leaseweb shall only Process Personal Data if and to the extent such Processing is required and permitted in the performance of the Sales Contract by Leaseweb (such as the performance of support), and on other legal grounds such as legitimate interests. If Leaseweb is under a legal obligation to Process the Personal Data. Leaseweb shall inform the Customer of such legal obligation unless it is prohibited by law or reasons of important public interest from doing so.

2.2 Processing of Personal Data by Processor shall only take place if and to the extent and for the time that such Processing is required in the performance of the Sales Agreement by Processor and the related legitimate interests. Processor will endeavour to arrange that only authorized personnel shall have access to the Personal Data.

2.3 Processor shall not retain the Personal Data of Controller longer than is necessary for (i) the performance of the Services; or (ii) complying with any statutory obligation of Processor.

3. SUBCONTRACTORS

3.1 Processor is entitled to sub-contract any of its obligations under this DPA, without the prior written approval of Controller. Upon request, a list of the third parties shall be provided to the Controller.

3.2 In case Processor engages sub-contractors in the performance of the DPA, Processor shall impose on them the data protection obligations as set forth in this DPA.

4. SECURITY

4.1 When Processing the Personal Data of Controller under this DPA, Processor shall take adequate technical and organisational precautions and measures. Whether the measures are sufficient and suitable, will be determined based on the state of the art, costs of implementation, the nature, scope, context and purposes of the Processing as well as the risk of such Processing. Processor shall ensure and procure that any third party engaged by or on behalf of Processor shall take adequate necessary technical and organisational precautions and measures.

4.2 The security measures as referred to in Clause 4.1 meet the requirements under the Data Protection Legislation, and in any case include the following certifications: ISO 27001, NEN7510, SOC1, PCI DSS, CISPE and EU-US Privacy Shield. Upon reasonable request, Processor shall provide an overview of the security measures in place. To safeguard the integrity of this security, such overview shall -necessarily- be general in nature.

5. NOTIFICATION DUTY

5.1 In case of a Data Breach Processor shall notify Controller without undue delay after discovery of such Data Breach. Such notification shall be in accordance with Clause 5.2.

5.2 Parties agree that Processor, in case of a Data Breach, shall - without undue delay - inform Controller in writing (e-mail is allowed) to Controller. Processor shall inform the following contact persons of Controller: [name], [title], [telephone], [email].
If any alterations are made by Controller with regards the above contact details, Controller will inform Processor directly. If Controller fails to do so, the (possibly negative) consequences thereof are borne by Controller.

5.3 Processor shall provide Controller in its notification with all necessary information, including but not limited to (i) the nature of the Data Breach, including the categories and approximate number of Data Subjects and records concerned; (ii) the contact at Processor who will liaise with Controller with respect to the Data Breach; (iii) the probable consequences of the Data Breach on the (processing of) the Personal Data; and (iv) the remediation measures taken to mitigate and contain the Data Breach.

5.4 Processor shall, at request thereto by Controller, cooperate with informing the competent Authority – which means the authority that is engaged to supervise the processing of Personal Data within the meaning of Article 4 paragraph 21 jo. Article 51 GDPR - and Data Subject(s) with respect to the (actual or suspected) Data Breach. Controller shall at its sole discretion determine whether to provide notification to the Data Subject, any third party or Authority and Processor shall not notify the Data Subject, any third party or Authority unless such disclosure by Processor is required by law.

6. TRANSFER OF PERSONAL DATA

6.1 Processor shall only Process Personal Data in countries outside the European Economic Area that ensure an adequate level of protection, in line with the applicable Data Protection Legislation. If Controller requests Processor to Process Personal Data outside the European

Economic Area, Controller represents that it has the legal authority and consents necessary to transfer the Personal Data in that manner.

7. AUDIT

7.1 Processor is frequently being audited by external parties to ensure it complies with relevant normative frameworks and controls within the Leaseweb Circle of Trust model. See https://www.leasewebLeaseweb.com/certifications for more information.

7.2 Controller has the right, upon its request and under the conditions as specified in this Clause 7, to have an independent auditor conduct an audit regarding the organisation of Processor, in order to establish whether or not Processor complies with the applicable Data Protection Legislation and the DPA.

7.3 Such an audit shall take place only after Controller has requested Processor to present it with an internal audit report; and if, after having reviewed such an internal audit report, Controller can substantiate why an additional external audit is justified. Such an external audit is justified if the internal audit report does not establish, or insufficiently establishes, whether or not Processor complies with the applicable Data Protection Legislation and the DPA. Controller may request an external audit once every two (2) years, giving Processor two (2) weeks' notice in advance, notwithstanding the compelling reason as referred to in Clause 7.4.

7.4 Processor will cooperate with the external audit upon request of Controller and provide Controller with all information that can reasonably be deemed relevant, within a reasonable period of time. Parties agree that a period of two (2) weeks is reasonable, unless a compelling reason requires more immediate action.

7.5 Prior to the external audit upon request of Controller, Parties shall establish in writing whether the results of such an audit shall be subject to review and discussion of Parties, or that the results will be accepted irrevocably. If it is established that Processor has failed to comply with the provisions of applicable Data Protection Legislation and the DPA, Processor shall take all reasonably necessary measures to ensure compliance going forward.

7.6 The costs of audits upon request of Controller, will be borne by Controller, unless the results of such an audit show that Processor has failed to comply with the provisions of applicable Data Protection Legislation and the DPA.

8. DATA SUBJECTS

8.1 In case a Data Subject wishes to exercise its rights under the Data Protection Legislation, Processor shall cooperate to the extent that can reasonably be expected of Processor to ensure Controller can comply with its statutory obligations in this respect.

8.2 If and when a Data Subject, in the course of exercising its rights under the Data Protection Legislation, reaches out directly to Processor, Processor shall forward such contact to Controller without undue delay and shall abstain from giving any substantive reply thereto, other than indicating the matter is being handled by Controller.

9. INDEMNIFICATION

9.1 Controller indemnifies Processor from and against all claims by third parties, including data subjects, asserted against Processor due to a breach of the Data Protection Legislation or other applicable regulations concerning the processing of Controller Personal Data, or the DPA, that is attributable to Controller or third parties engaged by Controller. If such breach causes a measure or fine to be imposed on Processor by the Authority, Controller shall also indemnify Processor for all costs resulting therefrom.

9.2 Controller shall take out insurance sufficient to cover any payment that may be required under this Clause 9 and provide Processor with the policy on request.

10. LIMITATION OF LIABLITY

10.1 Any liability of Processor is limited to the affected Services and to the amount (excluding VAT) invoiced by Processor under the Agreement and timely paid by Controller, in the three (3) months prior to the day on which the liability arises, with a maximum of twenty-five thousand euros (EUR 25.000,=) per damaging event or series of damaging events.

10.2 In no event shall Processor be liable under or in connection with DPA for any indirect, Data Breach or consequential damages (including but not limited to: lost opportunities, loss of turnover, profits or goodwill, loss, mutilation or destruction of data or data files, and damages for liability towards third parties).

10.3 All of Controller's claims on Processor, on whatever grounds, including but not limited to breach of DPA or tort, shall expire and cease to exist after a period of twelve (12) months following the day of the damaging event, if Controller fails to inform Processor of the existence of such claim(s) and has failed to bring the claim(s) before the authorized court within the aforementioned period of twelve (12) months.

11. TERM AND TERMINATION

11.1 The DPA shall become effective upon signing by both Parties or, if earlier, by execution thereof by either Party.

11.2 The term of the DPA is equal to the term of the Agreement. Parties agree upon a 'phase out-period' of one (1) month, during which the obligations of the DPA shall still be applicable after the Agreement has ended. The DPA cannot be terminated prematurely.

11.3 Upon termination or expiry of the Agreement for whatever reason, Processor shall delete all the Personal Data pertaining to the Customer, including copies thereof, unless Processor is required to retain such Personal Data under the applicable law. If required by law to retain a copy, Processor shall inform Controller what it is retaining and the legal reason why it needs to be retained, unless prohibited to do so by law.

11.4 The Clauses of the DPA that are intended to remain in force after the DPA has terminated or expired for whatever reason, shall remain in force after termination or expiration of the DPA, including but not limited to Clause 13 and this Clause 11.4.

12. MISCELLANEOUS

12.1 No change or amendment to or modification of the DPA shall be valid unless in writing and signed by both Parties.

12.2 Should any provision of the DPA be declared invalid for any reason, such decision will not affect the validity of any remaining provisions which will remain in force and effect. In any such event, Parties will endeavour to replace the invalid provision with a provision of equivalent effect.

13. APPLICABLE LAW AND COMPETENT COURT

13.1 This DPA and all matters regarding the construction, interpretation or enforcement thereof shall be governed by the laws of the Commonwealth of Virginia.

13.2 Any matters or disputes arising in connection with the DPA, its subject matter or the legal relationship between Processor and Controller shall be exclusively heard by the or federal courts of Prince William County, Virginia, USA.

For and on behalf of	For and on behalf of
Leaseweb USA, Inc.	[……]
_____	_____
Name:	Name:
Position:	Position:
Date:	Date:

ANNEX 1 –TECHNICAL AND ORGANISATIONAL MEASURES

Processor has implemented the following security measures in its organisation:

- Network segmentation
- Next generation firewalls
- Anti-virus software
- Full disk encryption of end-points
- Encrypted communication via SSL or VPN
- Security Information and Event Management solutions
- Dedicated Security Operating Centre
- Security Awareness training
- Segregation of duties
- Role-based access permissions (based on least-privilege)
- Secure disposal facilities of confidential information
- Periodic pen testing of public facing services
- Secure development training
- Integrated security monitoring during development
- Tools to enable employees to work secure (such as password managers)
- Physical security zones

Per application or communication, additional security measures can be implemented.

Processor is frequently being audited by external parties to ensure it complies with relevant normative frameworks and controls within the Leaseweb Circle of Trust model. See https://www.leaseweb.com/certifications for more information.